

DIN ISO/IEC 27001:2015-03 (D)

Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits- Managementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014)

Inhalt	Seite
Nationales Vorwort.....	3
Nationaler Anhang NA (informativ) Literaturhinweise	4
0 Einleitung	5
0.1 Allgemeines	5
0.2 Kompatibilität mit anderen Normen für Managementsysteme	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Kontext der Organisation	6
4.1 Verstehen der Organisation und ihres Kontextes	6
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	6
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	7
4.4 Informationssicherheitsmanagementsystem	7
5 Führung	7
5.1 Führung und Verpflichtung	7
5.2 Politik	8
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation.....	8
6 Planung	8
6.1 Maßnahmen zum Umgang mit Risiken und Chancen.....	8
6.2 Informationssicherheitsziele und Planung zu deren Erreichung	10
7 Unterstützung	11
7.1 Ressourcen	11
7.2 Kompetenz	11
7.3 Bewusstsein.....	11
7.4 Kommunikation	11
7.5 Dokumentierte Information	12
8 Betrieb	13
8.1 Betriebliche Planung und Steuerung	13
8.2 Informationssicherheitsrisikobeurteilung	13
8.3 Informationssicherheitsrisikobehandlung.....	13
9 Bewertung der Leistung	13
9.1 Überwachung, Messung, Analyse und Bewertung	13
9.2 Internes Audit	14
9.3 Managementbewertung	14
10 Verbesserung.....	15
10.1 Nichtkonformität und Korrekturmaßnahmen	15
10.2 Fortlaufende Verbesserung.....	15
Anhang A (normativ) Referenzmaßnahmenziele und -maßnahmen	16
Literaturhinweise	31